Navajo County

Incident Response Procedure	Created: 6/23/2015
Section of: Navajo County Security Procedures	Target Audience: Technical
CONFIDENTIAL	Page 1 of 6

1.0 Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Procedure is critical to successful recovery from an incident. This procedure covers all incidents that may affect the security and integrity of Navajo County's information assets, and outlines steps to take in the event of such an incident.

2.0 Purpose

This procedure is intended to ensure that Navajo County is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this procedure is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

3.0 Scope

The scope of this procedure covers all information assets owned or provided by Navajo County, whether they reside on the County network or elsewhere.

4.0 Procedure

4.1 Types of Incidents

A security incident, as it relates to Navajo County's information assets, can take one of two forms. For the purposes of this procedure a security incident is defined as one of the following:

- Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.
- Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain County information.

4.2 Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

Additionally, prior to an incident, Navajo County must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

Navajo County should continue to review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

Navajo County IT will participate in the annual emergency management exercise. A member of the IT staff will be part of the emergency management team to help coordinate any IT response to an incident.

4.3 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

4.4 Electronic Incidents

When an electronic incident is suspected, Navajo County's goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
2. Disable the compromised account(s) as appropriate.
3. Report the incident to the IT Director.
4. Backup all data and logs on the machine, or copy/image the machine to another system. Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?
5. Notify County management/executives as appropriate.

6. Contact an IT Security consultant as needed.
7. Determine how the attacker gained access and disable this access.
8. Rebuild the system, including a complete operating system reinstall.
9. Restore any needed data from the last known good backup and put the system back online.
10. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.
11. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the procedure adequate? What could be done differently?
12. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

4.5 Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at Navajo County.

4.5.1 Response

Establish the severity of the incident by determining the data stored on the missing device. Two important questions must be answered:

1. Was confidential data involved?
   a. If not, refer to "Loss Contained" below.
   b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
   a. If strong encryption was used, refer to "Loss Contained" below.
   b. If not, refer to "Data Loss Suspected" below.

4.5.2 Loss Contained

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Director. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

4.5.3 Data Loss Suspected

First, notify the IT Director, the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

4.6 Notification

If an electronic or physical security incident is suspected to have resulted in the loss of County Personally Identifiable Information data, notification of the public or affected entities might need to occur. First this must be discussed with the IT Director, the executive team and legal counsel to determine an appropriate course of action. If notification is deemed appropriate, it should occur in an organized and consistent manner.

4.7 Managing Risk

Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security procedure. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to Navajo County. IT staff will perform security vulnerability reviews on a periodic basis as directed by the IT Director. IT staff are members of security assessment groups and consortiums. Staff will continue these relationships and expand to other groups as the opportunities arise. These organizations provide training and support for managing risk in addition to the County’s internal training.

4.7.1 Risk Assessment

A formal risk assessment is a good way to manage risk of a security incident. A risk assessment may or may not be performed at the discretion of the IT Director and/or Executive Team. If an assessment is performed, it should be an accurate and thorough assessment of the potential risks (man-made and natural) and any vulnerabilities to the confidentiality, integrity, and availability of Navajo County's critical or confidential information.

4.7.2 Risk Management Program

A risk management program may be adopted if deemed appropriate by the IT Director and/or Executive Team. If implemented, the program should cover any risks known to Navajo County (possibly identified by a risk assessment), and insure that reasonable security measures are in place to mitigate those risks to an acceptable level.

4.8 Applicability of Other Procedures

This document is part of Navajo County's cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

5.0 Enforcement

This procedure will be enforced by the IT Director and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of County property (physical or intellectual) are suspected, Navajo County may report such activities to the applicable authorities.

6.0 Definitions

Encryption – The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Malware – Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

Mobile Device – A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

PDA – Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone – A mobile telephone that offers additional applications, such as PDA functions and email.

Trojan – Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Virus – Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

WEP – Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WPA – Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

7.0 Revision History

Revision 1.0, 6/23/2015
Revision 1.5, 9/24/2015
Revision 1.8, 6/08/2016